JOURNAL OF COMPLEXITY 9, 4–14 (1993)

Complexity of Bezout's Theorem

III. Condition Number and Packing

MICHAEL SHUB AND STEVE SMALE*

IBM T. J. Watson Research Center, Yorktown Heights, New York 10598-0218

Received September 23, 1992

DEDICATED TO JOSEPH F. TRAUB ON THE OCCASION OF HIS 60TH BIRTHDAY

1. INTRODUCTION

The best known example of a condition number is that for the problem of solving a linear system $Ax = b$. The condition number is $\kappa_A = \|A\| \|A^{-1}\|$, where an operator norm on the matrix A is used. It measures the sensitivity of output error relative to input error. Since $\kappa_A \geq 1$, $\log \kappa_A$ is positive and measure the "loss of precision."

For finding a root of a polynomial f, or solving $f(\zeta) = 0$, the condition number has been taken as $W_{f,\zeta} = 1/|f'(\zeta)|$ as in Demmel (1987) (see also the earlier accounts Wilkinson (1963) and Woźniakowski (1977)).

Again it measures sensitivity relative to input error. This condition number lacks certain naturality properties as invariance under the transformations $f \to \lambda f$, or $\zeta \to \alpha\zeta$ for $\lambda, \alpha \in \mathbb{C} - 0$. Moreover, $W_{f,\zeta}$ does not satisfy $W_{f,\zeta} \geq 1$.

For these and other reasons we are motivated to define a new notion of condition number $\mu(f, \zeta)$ of a polynomial at $\zeta \in \mathbb{C}$.

Our emphasis is on homogeneous polynomials but the ideas apply in general. See Bez I and Bez II (Shub and Smale, 1992) for a general account of how $\mu(f, \zeta)$ plays a role in the complexity theory of solving polynomial systems. Our present account is mainly self-contained.

Let $\mathcal{P}_d$ be the space of complex polynomials of one variable of degree less than or equal to d, and $\mathcal{H}_d$ homogeneous polynomials of exact degree

* Partly supported by NSF funds.

0885-064X/93 $5.00

d in 2 variables. There is a natural isomorphism $\mathcal{P}_d \to \mathcal{H}_d, f \to g$, given by $g(x, y) = \sum_0^d a_i x^i y^{d-i}$ where $f(x) = \sum_0^d a_i x^i$. The projective space of lines through the origin of $\mathbb{C}^2$ is denoted by $\mathcal{P}(\mathbb{C}^2)$. The zeros of $g \in \mathcal{H}_d$ are naturally considered as points of $P(\mathbb{C}^2)$.

Now we must define the derivative of $g \in \mathcal{H}_d$ at a point $u = (z, w) \in \mathbb{C}^2$ so that it can be inverted, and makes sense in projective space. This cannot be done purely algebraically.

Let $\langle u, v\rangle$ denote the standard Hermitian inner product between vectors $u, v \in \mathbb{C}^2$, and $\|u\| = \langle u, u\rangle^{1/2}$ be the associated norm on $\mathbb{C}^2$. The complex numbers supposed to be imbedded in $\mathbb{C}^2$ by $z \to (z, 1) \in \mathbb{C}^2$ and we write

$$\|z\|_1 = \|(z, 1)\| = (1 + |z|^2)^{1/2}.$$

A model for the tangent space at $u \in P(\mathbb{C})$ is

$$N_u = \{v \in \mathbb{C}^2 \mid \langle v, u\rangle = 0\}.$$

The *projective derivative* of $g \in \mathcal{H}_d$ at $u \in \mathbb{C}^2$ will be the restriction of $Dg(u)$: $\mathbb{C}^2 \to \mathbb{C}$ to $N_u \subset \mathbb{C}^2$. Write this as $D_P g(u)$: $N_u \to \mathbb{C}$. (Recall $Dg(u)$ $(a, b) = (\partial g/\partial z)(u)(a) + (\partial g/\partial w)(u)b$ if $u = (z, w)$.)

The reciprocal of the magnitude of $D_P g_{(u)}$ is the key ingredient of our notion of condition number.

LEMMA 1. *Let $g \in \mathcal{H}_d$ be the homogenization of $f \in \mathcal{P}_d$ and ζ be a simple root of f. Then*

$$|D_P g(\zeta, 1)| = \|\zeta\|_1 |f'(\zeta)|.$$

Proof. We may write f in the form $f(z) = a_d \prod_1^d (z - \zeta_i)$, $\zeta_1 = \zeta$. Then $g(z, w) = a_d \prod_1^d (z - \zeta_i w)$ and $f'(\zeta) = a_d \prod_2^d (z - \zeta_i)$. For the proof we may suppose $a_d = 1$ by rescaling. The line $N_{(\zeta,1)} \subset \mathbb{C}^2$ is one dimensional, contains the unit vector $(1, -\bar{\zeta})/\|\zeta\|_1$ and so

$$|D_P g(\zeta, 1)| = \frac{|Dg(\zeta, 1)(1, -\bar{\zeta})|}{\|\zeta\|_1} = \left|\frac{\partial g}{\partial z}(\zeta, 1) - \bar{\zeta}\frac{\partial g}{\partial w}(\zeta, 1)\right| \frac{1}{\|\zeta\|_1}$$

$$= \left|\prod_2^d (\zeta - \zeta_i) + \bar{\zeta}\zeta \prod_{i=2}^d (\zeta - \zeta_i)\right| \frac{1}{\|\zeta\|_1}$$

$$= (1 + |\zeta|^2)|f'(\zeta)| \frac{1}{\|\zeta\|_1} = \|\zeta\|_1 |f'(\zeta)|. \quad \blacksquare$$

Before we are able to define our condition number, a norm must be defined on $\mathcal{H}_d$.

The group of linear automorphisms of $\mathbb{C}^2$ which preserve the inner product is called the unitary group, $U(2)$. Thus if $u, v \in \mathbb{C}^2$, $\alpha \in U(2)$, then $\langle \alpha u, \alpha v \rangle = \langle u, v \rangle$. As in Kostlan (1987), Bez I, Bez II, we replace the customary norm on $\mathcal{H}_d$, defined by $\|g\|^2 = \sum |a_i|^2$, for $g(x, y) = \sum a_i x^i y^{d-i}$, by a weighted version to make it unitarily invariant. Thus define

$$\|g\| = \left(\sum_{i=0}^{d} |a_i|^2 \binom{d}{i}^{-1} \right)^{1/2}, \qquad g \in \mathcal{H}_d,$$

where $\binom{d}{i}$ is the binomial coefficient. Thus $\|g\|^2 = \langle g, g \rangle$ where $\langle h, g \rangle = \sum b_i \bar{a}_i \binom{d}{i}^{-1}$ if $h(z) = \sum_0^d b_j z^j w^{d-j}$. The unitary group $U(2)$ induces an action on $\mathcal{H}_d$ by sending g into the composition $g \circ \alpha^{-1}$ for $\alpha \in U(2)$. It can be shown that the Hermitian structure and hence the norm $\| \ \|$ on $\mathcal{H}_d$ is unitarily invariant in the sense $\langle h \circ \alpha^{-1}, g\alpha^{-1} \rangle = \langle h, g \rangle$. If $f \in \mathcal{P}_d$, define $\|f\|$ as equal to $\|g\|$ where g is the homogenization of f. Finally, we define the condition number for $g \in \mathcal{H}_d$, and $u \in \mathbb{C}^2$ by

$$\mu(g, u) = \frac{d^{1/2} \|g\| \, \|u\|^{d-1}}{|D_P g(u)|}.$$

The $d^{1/2}$ is a convenient normalization factor which eventually makes a certain formula more elegant. Note the following properties of $\mu(g, u)$:

(i) $\mu(\lambda g, u) = \mu(g, u)$ all $\lambda \neq 0 \in \mathbb{C}$;

(ii) $\mu(g, \lambda u) = \mu(g, u)$ all $\lambda \neq 0 \in \mathbb{C}$;

(iii) $\mu(g\alpha^{-1}, \alpha u) = \mu(g, u)$ all $\alpha \in U(2)$;

(iv) $\mu(g, u) \geq 1$ ($= \infty$ for u a double root of g).

(i) insures that μ is defined on $P(\mathcal{H}_d)$, the projective space of lines in $\mathcal{H}_d$. (ii) implies that μ is defined for u in $P(\mathbb{C}^2)$ and (iii) that μ is invariant under the unitary action on $\mathcal{H}_d \times \mathbb{C}^2$. (iv) implies that its log or loss of precision is non-negative.

Let $g \in \mathcal{H}_d$, $u = (z, w)$ with $g(u) = 0$. Differentiating this equation yields

$$\dot{u} = -D_P g(u)^{-1} \left(\sum_0^d \dot{a}_i z^i w^{d-i} \right),$$

where $\dot{u} \in N_u$ and the $\dot{a}_i$ can be considered as perturbations in the coefficients of g. It follows that $\mu(g, u)$ reflects the sensitivity of the solution u to an error in g. In fact, using unitary invariance it is not difficult to see that

$$\mu(g, u) = d^{1/2} \sup_{\|\dot{a}\| \leq 1} \|\dot{u}\|, \qquad \dot{a} = (\dot{a}_0, \ldots, \dot{a}_d)$$

where $\dot{u}$ is considered as tangent to $P(\mathbb{C}^2)$ at a and $\dot{a}$ is tangent to $P(\mathcal{H}_d)$ at f with the induced Hermitian structures.

In Bez I and Bez II, $\mu(g, z)$ is defined generally for systems $g\colon \mathbb{C}^{n+1} \to \mathbb{C}^n$ of homogeneous polynomials, with properties generalizing (i)–(iv).

In Bez I and Bez II a condition number theorem is proved which identifies the condition number with the reciprocal of a notion of distance to ill-posed problems.

If $f \in \mathcal{P}_d$, $\zeta \in \mathbb{C}$, define $\mu(f, \zeta) = \mu(g, (\zeta, 1))$ where g is the homogenization of f.

The condition number of $g \in \mathcal{H}_d$ (no ζ) is defined by

$$\mu(g) = \max_{\substack{u \\ g(u)=0}} \mu(g, u)$$

and so is ∞ if g has a double root. If $f \in \mathcal{P}_d$,

$$\mu(f) = \max_{\substack{\zeta \\ f(\zeta)=0}} \mu(f, \zeta).$$

EXAMPLE. For each $d = 1, 2, \ldots$ and fixed $a > 0$, let a polynomial $g \in \mathcal{H}_d$ be defined by

$$g_d(z, w) = z^d - a^d w^d.$$

A zero of g_d is $\zeta_a = (a, 1)$. One can use Lemma 1 to show

$$\mu(g_d, \zeta_a) = \frac{d^{1/2}(1 + a^2)^{(d-2)/2}(1 + a^{2d})^{1/2}}{(d - 1)a^{d-1}}.$$

By unitary invariance $\mu(g_d) = \mu(g_d, \zeta_a)$.

For each $a > 0$, $\mu(g_d)$ grows exponentially fast as a function of d. Thus one could say that $\{f_d\}$ is a poorly conditioned family of polynomials.

This has the following consequences. Versions of g_d are typically used to initiate homotopy methods for solving a polynomial equation, or a polynomial system of equations. See Bez I for the literature on this. The speed of the algorithm can be proved to depend on the conditioning of the homotopy (Bez I). But if the homotopy is poorly conditioned at time = 0, it is certainly poorly conditioned. This raises the question (to which this note is addressed), "does there exist a well-conditioned family $\{g_d\}_{d=1,2,\ldots}$ $g_d \in \mathcal{H}_d$, and if so can one find it?"

An answer to the first problem is provided by Bez II. Use the standard measure on the projective space of lines through 0 in $\mathcal{H}_d$, $P(\mathcal{H}_d)$, normalized to have total volume 1.

Then it follows easily from part (ii) of Theorem D of Bez II that for $0 < m < 1$ there is a subset $S_m \subset P(\mathcal{H}_d)$ of measure $1 - m$ such that for $g \in S_m$

$$\mu(g) \leq \left[\frac{d(d-1)^2}{m}\right]^{1/4}.$$

In particular there is a subset S of $P(\mathcal{H}_d)$ of volume 1/2 such that for $g \in S$

$$\mu(g) \leq d \qquad \text{all } d \geq 2.$$

This suggests

Main Problem. Find explicitly a family $\{g_d\}$, $g_d \in \mathcal{H}_d$ with $\mu(g_d) \leq d$.

In fact it seems difficult even to find such g_d with $\mu(g) \leq d^q$ any fixed q (as $q = 100$).

What does it mean "to find explicitly?" There are different levels of interpretation, along the lines of "giving a handy description." More formally, describe a polynomial time machine (as in Blum, Shub, and Smale, 1989) to output such g_d as a function of d.

The next section will relate the main problem to the Fekete theory of Transfinite Diameter, in its elliptic version in Tsuji (1959). This translates the problem to a kind of packing problem on S^2: Find a set of d points on S^2, no two of which are very close together.

This also brings our problem into good contact with problems of finding electrostatic equilibria on S^2, of Tomography, and distributions of points on the sphere as in Lubotzky, Phillips, and Sarnak (1986).

2. Elliptic Fekete Polynomials Are Well Conditioned

Let S^2 be the sphere of radius 1/2 centered at (0, 1/2) in $\mathbb{C} \times \mathbb{R} = \mathbb{R}^3$. If $z \in \mathbb{C}$, let $\hat{z}$ be the point in S^2 obtained from $(z, 1)$ by stereographic projection from (0,0). See Hille I (1962) for

Lemma 2. *For any* $z_1, z_2 \in \mathbb{C}$,

$$\|\hat{z}_1 - \hat{z}_2\| = \frac{|z_1 - z_2|}{(1 + |z_1|^2)^{1/2}(1 + |z_2|^2)^{1/2}}$$

$$\hat{z} = \frac{(z, 1)}{1 + |z|^2}.$$

Here $\| \|$ is the $\mathbb{R}^3$ norm.

One may consider S^2 as a model of $P(\mathbb{C}^2)$, and $\| \ \|$ a variant of the standard distance in $P(\mathbb{C}^2)$. In this way, some of this paper extends to n variables.

Let V_d be the maximum value of

$$\prod_{1 \le i < j \le d} \|x_i - x_j\| \qquad \text{over all } x_1, \ldots, x_d \in S^2.$$

The *elliptic Fekete points* (of order d) are a d-tuple $(x_1, \ldots, x_d)$ which realizes this maximum. By compactness, V_d and such $(x_1, \ldots, x_d)$ exist. By a rotation of S^2, we may suppose no x_i is (0, 0) and so there are $z_1, \ldots, z_d \in \mathbb{C}$ such that $\hat{z}_i = x_i$, $i = 1, \ldots, d$. Then for each d, $F_d(z) = \prod_1^d (z - z_i)$ is an *elliptic Fekete polynomial.*

Hille II (1962) has an account of the original Fekete theory and the elliptic version we use here may be found in Tsuji (1959). The sequence $\delta_d = V_d^{2/d(d-1)}$ is a decreasing function of d with limit as $d \to \infty$, the elliptic transfinite diameter, T.D., of S^2 according to Tsuji (1959). This number is $1/\sqrt{e}$. A main result of the Fekete–Tsuji (see Tsuji, 1959, p. 93) theory is the identification of T.D. with the elliptic capacity, and an elliptic Chebyshev constant, all proved for the general case of the points constrained to lie in some region of S^2.

For $f \in \mathcal{P}_d$ with zeros $z_1, \ldots, z_d$, define a continuous function $\hat{f}$: $S^2 \to \mathbb{R}$ by

$$\hat{f}(x) = \prod_{i=1}^{d} \|x - \hat{z}_i\|.$$

Moreover, for a zero $\zeta \in \mathbb{C}$ of f, let

$$\hat{f}_\zeta(x) = \frac{\hat{f}(x)}{\|x - \hat{\zeta}\|}.$$

With this notation, we will prove in Section 3.

PROPOSITION 1.

$$\frac{1}{\pi^{1/2}} \frac{\|\hat{f}\|_{L^2}}{\hat{f}_\zeta(\hat{\zeta})} \le \frac{V_d}{\prod_{k<l} \|\hat{z}_k - \hat{z}_l\|}.$$

Here we are using the usual L^2 norm for functions on S^2.

PROPOSITION 2.

$$\mu(f, \zeta) = \frac{\sqrt{d(d+1)}}{\pi^{1/2}} \frac{\|\hat{f}\|_{L^2}}{\hat{f}_\zeta(\hat{\zeta})}.$$

Our main result is an immediate consequence of these two propositions.

THEOREM. *For any polynomial* $f\colon \mathbb{C} \to \mathbb{C}$ *of degree* d *with zeros* $z_1, \ldots, z_d$, ζ *one of the* z_i,

(A) $\mu(f) = \mu(f, \zeta) \leq \sqrt{d(d+1)}\, V_d / \prod_{k<l} \|\hat{z}_k - \hat{z}_l\|$

(B) $\mu(F_d) = \mu(F_d, \zeta) \leq \sqrt{d(d+1)}$ (*elliptic Fekete polynomials are well conditioned*).

Since $\prod_{k<l} \|\hat{z}_k - \hat{z}_l\|$ tends to get smaller as some pair of points $\hat{z}_k$, $\hat{z}_l$ become close, the maximum gives some kind of well-spaced $\hat{z}_1, \ldots, \hat{z}_d$ on S^2. Thus the elliptic Fekete polynomials represent some kind of solution to a packing problem.

Part (B) of the theorem says that the elliptic Fekete polynomials satisfy the condition of the main problem (almost! $\sqrt{d(d+1)}$ instead of d). But they are not found explicitly in any sense.

One way of attacking the main problem would be to give and analyze an algorithm for maximizing the function $\Phi\colon (S^2)^d \to \mathbb{R}$ where $\Phi(x_1, \ldots, x_d) = \prod_{i<j} \|x_i - x_j\|$. However, this may not be so easy since there are saddle points of index d (on a great circle in S^2, evenly space, d points, $x_1, \ldots, x_d$). Also the various symmetries that Φ possesses will confuse the picture.

3. Proof of Propositions 1 and 2

First we give the proof of Proposition 1. Let f, z_i, ζ be as in Section 2 with $\zeta = z_j$ say. First note:

$$\prod_{k<l} \|\hat{z}_k - \hat{z}_l\| = \prod_{\substack{k<l \\ k,l \neq j}} \|\hat{z}_k - \hat{z}_l\| \hat{f}_\zeta(\hat{\zeta}). \tag{*}$$

Thus by maximality of V_d, for $z = z_j$,

$$\hat{f}_\zeta(\hat{z}) \prod_{\substack{k<l \\ k,l \neq j}} \|\hat{z}_k - \hat{z}_l\| \leq V_d$$

and in fact for any z this is true for the same reason. Using (*) again we obtain

$$\hat{f}_\zeta(\hat{z}) \frac{\prod_{k<l} \|\hat{z}_k - \hat{z}_l\|}{\hat{f}_\zeta(\hat{\zeta})} \leq V_d.$$

Now square, integrate over $\hat{z} \in S^2$, and take the square root to obtain:

$$\left(\frac{1}{\mathrm{Vol}(S^2)}\right)^{1/2}\left(\int \hat{f}(\hat{z})^2\right)^{1/2}\frac{\Pi_{k<l}\|\hat{z}_k - \hat{z}_l\|}{\hat{f}_\xi(\hat{\xi})} \leq V_d.$$

Since $\mathrm{Vol}(S^2) = \pi$. This yields Proposition 1.

For the preparation of the proof of Proposition 2, we prove some lemmas.

LEMMA 3. *Let* $S^3 = \{(z, w) \in \mathbb{C}^2 | \ |z|^2 + |w|^2 = 1\}$. *Then*

$$\int_{S^3} |z|^{2k}|w|^{2l} = 2\pi^2\frac{\Gamma(k+1)\Gamma(l+1)}{\Gamma(k+l+2)}.$$

Proof. As in Bez II,

$$\begin{aligned}\int_{S^3} |z|^{2k}|w|^{2l} &= 2\pi\int_{D^2} |z|^{2k}(1-|z|^2)^l \\ &= 2\pi^2\int_0^1 (s^2)^k(1-s^2)^l\,2s\,ds \\ &= 2\pi^2\frac{\Gamma(k+1)\Gamma(l+1)}{\Gamma(k+l+2)}.\end{aligned}$$

Let $\langle f, g\rangle' = (\int_{S^3} f\bar{g})^{1/2}$ be the L_2 Hermitian structure on $\mathcal{H}_d$. $\langle fu, gu\rangle' = \langle f, g\rangle'$ for a unitary transformation, so we know by the uniqueness of unitarily invariant inner products (see Kostlan, 1987) that $\langle f, g\rangle'$ and $\langle f, g\rangle$ differ by a multiplicative constant.

LEMMA 4. *For* $f, g \in \mathcal{H}_d$

$$\langle f, g\rangle' = \frac{2\pi^2}{d+1}\langle f, g\rangle.$$

Proof. It suffices to check the equality on a monomial $z^i w^{d-i}$. By Lemma 3

$$\begin{aligned}\langle z^i w^{d-i}, z^i w^{d-i}\rangle' &= \int_{S^3} |z|^{2i}|w|^{2(d-i)} \\ &= 2\pi^2\frac{\Gamma(i+1)\Gamma(d-i+1)}{\Gamma(d+2)} \\ &= \frac{2\pi^2}{d+1}\left(\frac{i!(d-i)!}{d!}\right) \\ &= \frac{2\pi^2}{d+1}\langle z^i w^{d-i}, z^i w^{d-i}\rangle,\end{aligned}$$

by the definition of $\langle,\rangle$.

Let $J: S^3 \to S^2$ be the composition $(z, w) \to ((z/w), 1) \to \widehat{z/w}$ if $w \neq 0$ and $J(1, 0) = (0, 0) \in S^2$, where S^2 is represented as in Section 2. Let $z \in \mathcal{P}_d$ have zeros $z_1, \ldots, z_d$, and $g \in \mathcal{H}_d$, be the homogenization of f. Then

LEMMA 5.

$$|g(z, w)| = \hat{f}(J(z, w)) \prod_{j=1}^{d} \|z_j\|_1.$$

Proof. Use Lemma 2. Then

$$\begin{aligned}\prod_j \|z_j\|_1 \hat{f}(J(z, w)) &= \prod_j \left\| \frac{\hat{z}}{w} - \hat{z}_j \right\| \|z_j\|_1 \\ &= \prod_j \frac{|z/w - z_i|}{\|z_j\|_1 (1 + |z/w|^2)^{1/2}} \|z_j\|_1 \\ &= \prod_j |z - z_j w| = |g(z, w)|.\end{aligned}$$

LEMMA 6. *The map $J: S^3 \to S^2$ has as fibers, unit circles, and the normal Jacobian of J is* 1. *(It is the Hopf map.) Thus*

$$\int_{S^3} \varphi J = 2\pi \int_{S^2} \varphi$$

for a continuous function $\varphi: S^2 \to \mathbb{R}$.

The last sentence is essentially the Fubini Theorem or the co-area formula. For the proof first note that

$$J(z, w) = \overline{w}(z, w) \in S^2 \subset \mathbb{C} \times \mathbb{R} = \mathbb{R}^3$$

since $\widehat{z/w} = (z/w, 1)/1 + |z/w|^2 = (\overline{w}z, w\overline{w})$ using Lemma 2.

Then $J(\rho^{i\theta}a, \rho^{i\theta}b) = \rho^{-i\theta}\overline{b}(\rho^{i\theta}a, \rho^{i\theta}b) = \overline{b}(a, b)$. So J respects the S^1 action. Differentiating J at (a, b) on the tangent vector (u, v) gives $\overline{v}(a, b) + \overline{b}(u, v)$. Applying this to the normal to (a, b), $(-\overline{b}, \overline{a})$ gives

$$a(a, b) + \overline{b}(-\overline{b}, \overline{a}) = (a^2 - \overline{b}^2, ab + \overline{b}\overline{a}).$$

The length squared of this vector is 1. ∎

LEMMA 7. *With f, g as above $\|g\|_{L^2} = \|\hat{f}\|_{L^2} \sqrt{2\pi}\, \Pi_j \|z_j\|_1$.*

Proof. Use Lemma 5 to see

$$\|g\|_{L^2} = \prod_j \|z_j\|_1 \left(\int_{S^3} \hat{f}(J(z, w))^2 \right)^{1/2}.$$

Now apply Lemma 6 with $\varphi = \hat{f}^2$.

Let us now proceed to the proof of Proposition 2.

Let $f \in \mathcal{P}_d$ and ζ be a zero as in Section 2. From the definition of condition number and Lemma 1, we have

$$\mu(f, \zeta) = \frac{d^{1/2}\|f\| \, \|\zeta\|_1^{d-1}}{\|\zeta\|_1 |f'(\zeta)|}.$$

By Lemma 2, with $z_1, \ldots, z_d$ the zeros of f, and $\zeta = z_j$ some j,

$$\begin{aligned} |f'(\zeta)| &= \prod_{l \neq j} |\zeta - z_l| \\ &= \left(\prod_{l \neq j} \|\hat{\zeta} - \hat{z}_l\| \right) \|\zeta\|_1^{d-1} \prod_{l \neq j} \|z_l\|_1 \\ &= \hat{f}_\zeta(\hat{\zeta}) \|\zeta\|_1^{d-1} \prod_{l \neq j} \|z_l\|_1. \end{aligned}$$

Thus

$$\mu(f, \zeta) = \frac{d^{1/2}\|f\|}{\|\zeta\|_1 \hat{f}_\zeta(\hat{\zeta}) \prod_{l \neq j} \|z_l\|_1}.$$

Using Lemma 4 this becomes

$$\mu(f, \zeta) = \frac{\sqrt{d(d+1)}}{\sqrt{2}\pi} \frac{\|g\|_{L^2}}{\|\zeta\|_1 \hat{f}_\zeta(\hat{\zeta}) \prod_{l \neq j} \|z_l\|_1}.$$

Now apply Lemma 7 to obtain

$$\begin{aligned} \mu(f, \zeta) &= \frac{\sqrt{d(d+1)}\sqrt{2\pi}}{\sqrt{2}\pi} \frac{\|\hat{f}\|_{L^2} \prod_k \|z_k\|_1}{\hat{f}_\zeta(\hat{\zeta}) \|\zeta\|_1 \prod_{l \neq j} \|z_l\|_1} \\ &= \frac{\sqrt{d(d+1)}}{\pi^{1/2}} \frac{\|\hat{f}\|_{L^2}}{\hat{f}_\zeta(\hat{\zeta})}, \end{aligned}$$

proving Proposition 2.

REFERENCES

BLUM, L., SHUB, M., AND SMALE, S. (1989), On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines, *Bull. Amer. Math. Soc.* **21**, 1–46.

DEMMEL, J. (1987), On condition numbers and the distance to the nearest ill-posed problem, *Numer. Math.* **51**, 251–289.

HILLE, E. (1962), "Analytic Function Theory, I and II," Ginn, Boston.

KOSTLAN, ERIC (1987), Random polynomials and the statistical fundamental theorem of algebra, preprint, Univ. of Hawaii.

LUBOTZKY, A., PHILLIPS, R., AND SARNAK, P. (1986), Hecke operators and distributing points on the sphere I, *Comm. Pure Appl. Math.* **VXXXIX,** 149–186.

SHUB, M., AND SMALE, S. (1991), Complexity of Bezout's Theorem I: Geometric aspects, *J. Amer. Math. Soc.*, to appear.

SHUB, M., AND SMALE, S. (1992), Complexity of Bezout's Theorem II: Volumes and probabilities, *in* "Computational Algebraic Geometry," (F. Eyssette and A. Galligo, Eds.) Birkhauser, to appear.

TSUJI, M. (1959), "Potential Theory in Modern Function Theory," Maruzen Co., Ltd., Tokyo.

WILKINSON, J. (1963), "Rounding Errors in Algebraic Processes," Prentice–Hall, Englewood Cliffs, N.J.

WOŹNIAKOWSKI, H. (1977), Numerical stability for solving non-linear equations, *Numer. Math.* **27,** 373–390.